



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/821,584	03/29/2001	James F. Riordan	CH920000010US1	3499
48813	7590	07/09/2008	EXAMINER	
LAW OFFICE OF IDO TUCHMAN (YOR) ECM #72212 PO Box 4668 New York, NY 10163-4668			PYZUCHA, MICHAEL J	
ART UNIT	PAPER NUMBER	2157		
NOTIFICATION DATE		DELIVERY MODE		
07/09/2008		ELECTRONIC		

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

pair@tuchmanlaw.com
idotuchman@gmail.com

Office Action Summary	Application No.	Applicant(s)
	09/821,584	RIORDAN ET AL.
	Examiner	Art Unit
	MICHAEL PYZOWA	2137

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If no period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).

Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(o).

Status

1) Responsive to communication(s) filed on 30 April 2008.

2a) This action is **FINAL**. 2b) This action is non-final.

3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4) Claim(s) 30-38 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5) Claim(s) _____ is/are allowed.

6) Claim(s) 30-38 is/are rejected.

7) Claim(s) _____ is/are objected to.

8) Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9) The specification is objected to by the Examiner.

10) The drawing(s) filed on _____ is/are: a) accepted or b) objected to by the Examiner.

 Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

 Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a) All b) Some * c) None of:

- Certified copies of the priority documents have been received.
- Certified copies of the priority documents have been received in Application No. _____.
- Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) Notice of References Cited (PTO-892)
 2) Notice of Draftsperson's Patent Drawing Review (PTO-948)
 3) Information Disclosure Statement(s) (PTO/SB/08)
 Paper No(s).Mail Date _____

4) Interview Summary (PTO-413)
 Paper No(s).Mail Date. _____

5) Notice of Informal Patent Application
 6) Other: _____

DETAILED ACTION

1. Claims 30-38 are pending.
2. Amendment filed 04/30/2008 has been received and considered.

Claim Rejections - 35 USC § 101

3. The rejection under 35 U.S.C. 101 has been withdrawn based on the filed amendment.

Claim Rejections - 35 USC § 103

4. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.
5. Claims 30-38 are rejected under 35 U.S.C. 103(a) as being unpatentable over Boroughs et al. (US 6834350) in view of Fujiyama et al. (US 6971026).

As per claims 30 and 33, Boroughs et al. discloses a security system comprising: an activation token identifying system characteristics and specifying a threat and at least one preset activation measure, wherein a system characteristic is one of the group of a hardware system, a service, a configuration of a service, a service execution platform, and a service session (see column 2 line 62 through column 3 line 34); a first system comprising a processor, the first system configured to at least review security and vulnerability information from information publishers and to provide the activation token based on filtered security and vulnerability information (see column 2 line 59 through column 3 line 10); and a second system configured to determine whether the

activation token is relevant by checking if actual characteristics at the second system correspond to the system characteristics identified by the activation token, the second system further configured to transform the activation token into at least one activation measure if the activation token is considered relevant by the second system the activation measure configured to modify services executing at the second system (see column 3 lines 35-67 and column 4 lines 1-5) wherein the first system is further configured to automatically filter the security and vulnerability information relevant to the system characteristics identified by the activation token (see column 2 line 59 through column 3 line 10 and Figure 17).

Boroughs et al. fail to explicitly disclose including a threat level within the activation token.

However, Fujiyama et al. teaches including a trust level with an activation token (see figures 2-5 and column 7 line 54 through column 8 line 55).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to include trust levels with the activation tokens of Boroughs et al.

Motivation to do so would have been to distinguish between the types of threats (see figures 2-5 and column 7 line 54 through column 8 line 55).

As per claim 31, the modified Boroughs et al. and Fujiyama et al. system discloses cryptographic means configured to verify at the second system that the first system is a trusted service (see Boroughs et al. column 3 lines 55-67).

As per claim 32, the modified Boroughs et al. and Fujiyama et al. system discloses reporting means configured to report to a system administrator of the second

system any activation measure taken by the second system (see Boroughs et al. column 2 lines 59-67).

As per claim 34, the modified Boroughs et al. and Fujiyama et al. system discloses a list of trusted service providers from whom activation tokens are accepted by the second system (see Fujiyama et al. column 8 lines 13-39).

As per claims 35 and 36, the modified Boroughs et al. and Fujiyama et al. system discloses a preset activation measure is one of shutting down a service affected by the specified threat level and reconfiguration of the service (see Fujiyama et al. Figure 3 column 202).

As per claim 38, the modified Boroughs et al. and Fujiyama et al. system fails to explicitly disclose that the at least one preset activation measure is alerting a system administrator.

However, Official Notice is taken that at the time of the invention it would have been obvious to alert a system administrator.

Motivation to do so would have been so that the system administrator knows to take action.

6. Claim 37 is rejected under 35 U.S.C. 103(a) as being unpatentable over the modified Boroughs et al. and Fujiyama et al. system as applied to claim 30 above, and further in view of Pearson (US 6990591).

As per claim 37, the modified Boroughs et al. and Fujiyama et al. system fails to explicitly disclose installing a patch as an activation measure.

However, Pearson teaches installing a patch (see column 13 lines 4-15).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to install a patch as one of the activation measures of the modified Boroughs et al. and Fujiyama et al. system.

Motivation to do so would have been to update the attack signature list (see Pearson column 13 lines 4-15).

Response to Arguments

7. Applicant's arguments filed 04/30/2008 have been fully considered but they are not persuasive. Applicant argues that Boroughs fails to disclose "a first system comprising a processor, the first system configured to at least review security and vulnerability information form information publishers and to provide the activation token based on filtered security and vulnerability information"; and fails to disclose "a second system configured to determine whether the activation token is relevant by checking if actual characteristics at the second system correspond to the system characteristics identified by the activation token, the second system further configured to transform the activation token into at least one activation measure if the activation token is considered relevant by the second system the activation measure configured to modify services executing at the second system"; Boroughs teaches away from a combination with Fujiyama; claim 31 is allowable for the reasons put forth above; Boroughs fails to teach the limitations of claim 32; claim 33 is allowable for the reasons put forth above; the combination of Boroughs and Fujiyama fails to teach the limitations of claims 34-36 and claims 37 and 38 are allowable for the reasons put forth above.

With respect to Applicant's argument that Boroughs fails to disclose "a first system comprising a processor, the first system configured to at least review security and vulnerability information from information publishers and to provide the activation token based on filtered security and vulnerability information", in column 2 lines 59-67 Boroughs describes a distribution (i.e. activation token). These distributions are prepared by network security experts and contain information describing newly-discovered network attacks (i.e. security and vulnerability information). This information can be obtained in one of two ways, either the experts find the attack themselves or receive information from one or more other entities. In the first case the experts themselves are the "information publishers" otherwise the other entities are the information publishers. Furthermore, in order for the experts to create and distribute the distribution with information and software, the must be part of a system that has at least one processor. Therefore, Boroughs teaches the first system of claim 30.

With respect to Applicant's argument that Boroughs fails to disclose "a second system configured to determine whether the activation token is relevant by checking if actual characteristics at the second system correspond to the system characteristics identified by the activation token, the second system further configured to transform the activation token into at least one activation measure if the activation token is considered relevant by the second system the activation measure configured to modify services executing at the second system", in column 3 lines 35-67 and column 4 lines 1-5 Boroughs describes a system that has a facility and subscribers, these entities combine to form the "second system" of claim 30. Therefore, the facility determines which

distributions are useful to each subscriber and sends them to each subscriber who then facilitates the application of the distribution (i.e. transforming the activation token to modify services of the second system). Therefore, Boroughs teaches the second system of claim 30.

With respect to Applicant's argument that teaches away from a combination with Fujiyama, the fact that Boroughs teaches always installing the distribution does not teach away from the selective installation of Fujiyama. Boroughs already teaches selectively installing certain distributions based on system characteristics, therefore it would be obvious to one of ordinary skill in the art to add the further selection based on security level as taught by Fujiyama in order to distinguish between types of threats. Therefore, Boroughs does not teach away from the combination and the combination is proper.

Applicant's argument that claim 31 is allowable for the reasons put forth above is moot in view of the above response.

With respect to Applicant's argument that Boroughs fails to teach the limitations of claim 32, Boroughs discloses alerting a user based on the received distribution (see column 4 lines 1-5) and further as shown in column 2 lines 56-67 the user can be an administrator. Therefore, Boroughs teaches the limitations of claim 32.

Applicant's argument that claim 33 is allowable for the reasons put forth above is moot in view of the above response.

With respect to Applicant's argument that the combination of Boroughs and Fujiyama fails to teach the limitations of claims 34-36, as per claim 34, Fujiyama FIG 16

shows multiple databases containing the security measures and the system must choose one of these databases, if these were not trusted databases the security of the system would fail. As per claim 35, the system of Fujiyama shuts down a service based on the security level (i.e. increasing the security). In other words if the security would be increased a certain amount (i.e. by reducing the threat level) the service would be shut down. As per claim 36, Fujiyama teaches reconfiguring the functionality of a service, similarly to the shutting down of a service. Therefore the combination teaches the limitations of claims 34-36.

Applicant's argument that claims 37 and 38 are allowable for the reasons put forth above is moot in view of the above response.

Conclusion

8. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to MICHAEL PYZOCHA whose telephone number is (571)272-3875. The examiner can normally be reached on Monday-Thursday, 7:00am - 4:30pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Emmanuel L. Moise/

Supervisory Patent Examiner, Art Unit 2137